BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 30 577.3

Anmeldetag: 05. Juli 2002

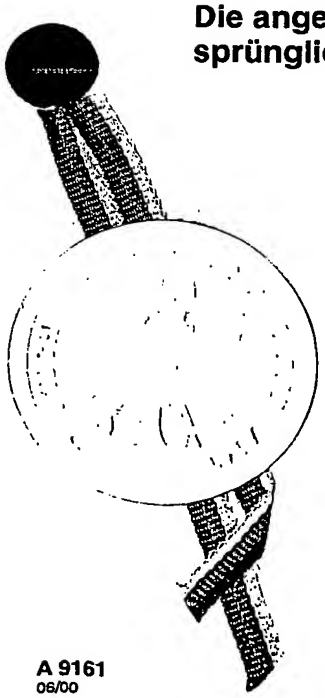
Anmelder/Inhaber: Continental Teves AG & Co oHG, Frankfurt am Main/DE

Bezeichnung: Verfahren zum Überwachen der Funktion und Erhöhen der Betriebssicherheit eines sicherheitsrelevanten Regelungssystems

IPC: G 05 B, G 01 M

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 06. Februar 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag



A 9161
06/00
EDV-L

Continental Teves AG & Co. oHG

05.07.2002
P 10461

Verfahren zum Überwachen der Funktion und Erhöhen der Betriebssicherheit eines sicherheitsrelevanten Regelungssystems

Die Erfindung bezieht sich auf ein Verfahren zum Überwachen der Funktion und zum Erhöhen der Betriebssicherheit eines komplexen sicherheitsrelevanten Regelungssystems sowie zum Erkennen und Auswerten von Systemfehlern.

Sicherheitsrelevante Systeme, zu denen Kraftfahrzeugregelungssysteme, wie ABS, ASR, ESP, „Brake-By-Wire"-Systeme (EHB,EMB), „Steering-By-Wire"-Systeme etc. zählen, erfordern Maßnahmen zur Sicherung einer definierten Funktionsweise auch im Falle erkannter Systemfehler. Es ist oft nicht möglich, einen erkannten Fehler im Normalbetrieb direkt einer Systemkomponente zuzuordnen. Solche Fehler, auch Gruppenfehler genannt, tragen meistens nur die Aussage, dass eine bestimmte physikalische Größe im System nicht eingehalten werden konnte. Erst die Durchführung spezieller Tests (auch Fehlerlokalisierungen genannt) ermöglicht es, die fehlerhafte Systemkomponente auszumachen (Umwandlung des Gruppenfehlers in einen Einzelfehler) und die passende Fehlerauswirkung (Systemdegradation) herbeizuführen.

Bevor die Fehlerlokalisierung erfolgreich abgeschlossen wird (unter Umständen tritt dieses Ereignis verspätet oder nie ein aufgrund z.B. Unterspannung oder früherer Fehler, die die Nutzung der für die Testdurchführung notwendiger Systemkomponenten ausschließen) befindet sich das System im undefinierten Zustand: man hat Kenntnis vom Fehlerzustand genommen, ist

aber nicht in der Lage, die passende Systemauswirkung herbeizuführen.

Der Erfindung liegt daher die Aufgabe zugrunde, beim Auftreten von Systemfehlern in Regelungssystem der hier in Rede stehenden Art in jeder Phase, auch bereits vor der Identifizierung des Einzelfehlers, das System in einem definierten Zustand zu halten und die Auswirkungen des Fehlers zu minimieren.

Die Lösung dieses Problems wird heute gesucht in diversen Fehleranalyseverfahren, die als Ergebnis der Erstfehlerbetrachtung eine Entscheidungsmatrix „Fehler->Systemauswirkung" liefern. Gruppenfehler gehören hierbei zu besonders schweren Analysefällen, da sie auf Fehler vieler Systemkomponenten gleichzeitig zurück führen können. Somit liegt die Findung einer zufriedenstellenden pauschalen Systemdegradationsstufe für einen Gruppenfehler oft nicht im menschlichen Ermessen. Der andere Nachteil dieses Ansatzes besteht darin, dass der Übergang von der pauschalen zu der feinen Einzelfehlerauswirkung nur nach dem erfolgreichen Abschluss der Fehlerlokalisierung möglich ist. Verzögert sich die Lokalisierung aufgrund von temporären Ereignissen oder wird sie aufgrund früher aufgetretener Fehler gar verhindert, so kommt die pauschale und meist schwerwiegende Systemdegradation zum Dauereinsatz. Dies wirkt sich wiederum negativ aus auf die Systemverfügbarkeit und -sicherheit.

Das erfindungsgemäße Verfahren beruht auf folgenden Überlegungen:
Die Ergebnisse der Erstfehleranalyse (beschränkt auf „echte" Komponentenfehler - unter Ausschluss der Gruppenfehler) eines sicherheitsrelevanten Systems verbergen heute ungenutzte In-

formationen, die sich im Gruppenfehlerfall nutzen lassen, um die Systemverfügbarkeit und -sicherheit zu erhöhen.

Im Folgenden wird ein auf den Ergebnissen der Erstfehleranalyse (beschränkt auf „echte" Komponentenfehler) basiertes Verfahren für den Einsatz in technischen Anwendungen beschrieben, das die Möglichkeit bietet, die Systemdegradation eines beliebigen sicherheitskritischen Systems während der aufgrund aufgetretener Gruppenfehler laufenden Lokalisierungen dynamisch zu minimieren. Dieses in jeder Techniksparte anwendbare Verfahren erhöht erheblich die Systemverfügbarkeit und gewährleistet letztendlich die Systemsicherheit, im Gegensatz zu den heute gängigen Verfahren, die sich auf die schwer definierbare pauschale Auswirkung der Gruppenfehler stützen.

Beschreibung:
Die Erstfehleranalyse (beschränkt auf „echte" Komponentenfehler) herkömmlicher Fehleranalysemethoden definiert die System- bzw. Komponentenauswirkung für jeden Einzelfehler.

Es wird hiermit vorgeschlagen, die System- bzw. Komponentenauswirkung eines Gruppenfehlers als Superposition der Auswirkungen aller Einzelfehler zu definieren, die als Ergebnis der korrelierten Fehlerlokalisierungen in Frage kommen.

Es wird des weiteren vorgeschlagen, die Auswirkung der Einzelfehler, die im Laufe der Fehlerlokalisierung als Fehlerquelle ausgeschlossen wurden, aus der System- bzw. Komponentenauswirkung des Gruppenfehlers ebenfalls auszuschließen. Es wird damit erreicht, dass im Laufe der Fehlerlokalisierung die Systemdegradation aufgrund eines Gruppenfehlers dauernd und fließend minimiert wird, bis die Ebene des erkannten Einzelfehlers erreicht wird. Wird die Lokalisierung aufgrund

temporärer Ereignisse verzögert oder aufgrund früherer Fehler gar abgebrochen beschränkt sich die Systemdegradation auf die Auswirkungen der (noch) nicht ausgeschlossenen Einzelfehlern.

Beispiel 1 (siehe Figur 1): Der aufgetretene Gruppenfehler GF löst drei parallel laufende Lokalisierungen L11, L21 und L31 aus. Jede dieser Lokalisierungen kann im nächsten Schritt zu jeweils 2 Einzelfehlern führen. Die Systemdegradation wird vorm Abschluss des ersten Lokalisierungsschritts als Superposition der Auswirkungen der Einzelfehler F1 - F6 berechnet.

Beispiel 2 (siehe Figur 2). Der erste Lokalisierungsschritt ist abgeschlossen: Lokalisierungen L11 und L31 haben keine Auffälligkeiten gemeldet; Einzelfehler F1, F2, F5 und F6 sind ausgeschlossen. Lokalisierung L21 hat hingegen ein positives Ergebnis gebracht. Im zweiten Schritt wird die Lokalisierung fortgesetzt zwecks Ergebnisverfeinerung. Die Systemdegradation wird vorm Abschluss des zweiten Lokalisierungsschritts als Superposition der Auswirkungen der Einzelfehler F3 und F4 berechnet. Die Systemverfügbarkeit hat sich erhöht.

Beispiel 3 (siehe Figur 3). Der zweite Lokalisierungsschritt ist abgeschlossen: Einzelfehler F4 ist ausgeschlossen, die Ursache für den Gruppenfehler GF ist der Einzelfehler F3. Die Systemdegradation ergibt sich direkt aus der Auswirkung des Einzelfehlers F3.

Das vorgeschlagene Verfahren bringt, im Vergleich zum bisherigen Verfahren unter anderem folgende Vorteile:

Die Auswirkung eines Gruppenfehlers ergibt sich automatisch aus der Summe der leicht definierbaren Auswirkungen für kor-

relierte Einzelfehler - Fehleranalyse für Gruppenfehler entfällt
Die Auswirkung eines Gruppenfehlers wird abgeschwächt mit dem Fortgang der Lokalisierungen - das System erfährt dynamisch eine erhebliche Steigerung der Verfügbarkeit und Sicherheit.

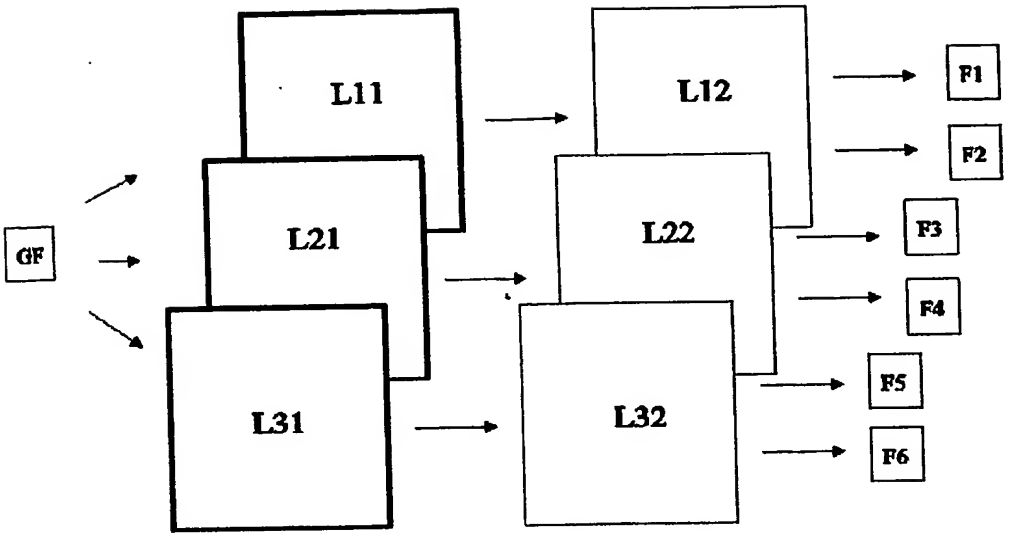
Der Fall, dass ein Gruppenfehler nicht zu Ende lokalisiert werden konnte, bedarf keiner gesonderten Behandlung

Patentanspruch:

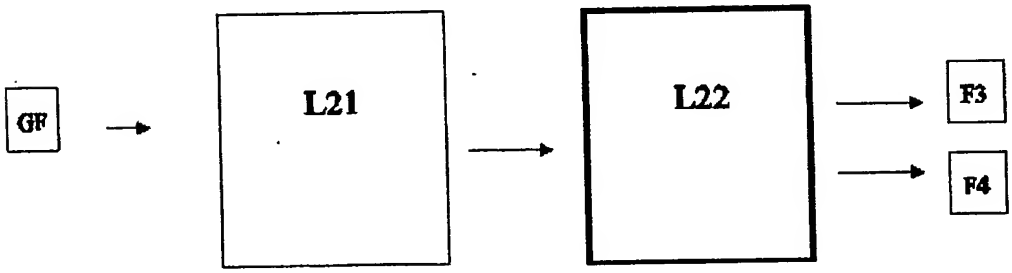
Verfahren zum Überwachen der Funktion und Erhöhen der Betriebssicherheit eines sicherheitsrelevanten Regelungssystems, z.B. eines Kraftfahrzeugregelungssystems, wie eines ABS, ASR, ESP, eines „Brake-By-Wire"-Systems (EHB,EMB), eines „Steering-By-Wire"-Systems etc., sowie zum Erkennen und Auswerten von Systemfehlern,

gekennzeichnet durch die Schritte:

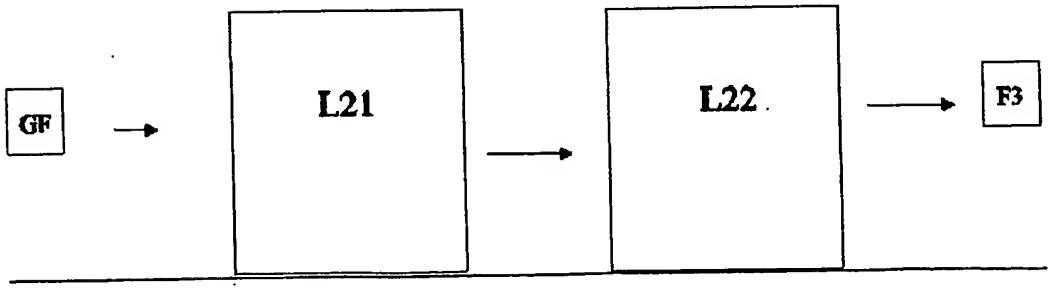
- Erkennen eines Systemfehlers und Bewertung als Gruppenfehler,
- Herbeiführen einer vollständigen oder dem Gruppenfehler entsprechenden teilweisen Systemdegradation oder Einschränkung der Systemfunktion bzw. Systemverfügbarkeit,
- Eingrenzung des Systemfehlers bzw. der Fehlerquelle durch Tests, logische Verknüpfung der Testsergebnisse, Plausibilitätsbetrachtungen etc.
- schrittweise Erhöhung der Systemverfügbarkeit in Abhängigkeit von dem Ergebnis der einzelnen Schritte zur Eingrenzung bzw. Lokalisierung des Systemfehlers oder der Fehlerquelle.



Figur 1



Figur 2



Figur 3